Safeguard Computer Security Evaluation Matrix (SCSEM)

GenTax Application
v6.0

Release IV

October 30, 2008

Internal Revenue Service

Tester: *Insert Tester Name*
Date: *Insert Date(s) Testing Occurred*
Location *Insert Location testing was conducted*
Agency POC(s): *Insert each Agency interviewee(s) name, address, phone number and email address.*
Hostname(s): *Insert the hostnames of the device(s) and the purpose of each device.*

Test ID	NIST ID (800-53)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
1	AC-2	Checks to see if the organization manages information system accounts, including establishing, activating, modifying, reviewing, and disabling accounts. The organization reviews information system accounts to ensure that existing accounts are being controlled properly.	1. [GTSYS] select * from tblUser where flngVer = 0 and fdtmStart < GetDate() and fdtmEnd > GetDate() Randomly choose users from scripted list of results. Verify the selected users are still active users that require GenTax application access. 2. Interview system or security administrator to verify how often the GenTax account list is reviewed for potential revision.	1. No accounts exist for individuals that are no longer associated with the organization, or no longer require access to the GenTax application. 2. User accounts are reviewed at least annually to ensure accounts are necessary and that account privileges are assigned correctly. Account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know/need-to-share changes.			
2	AC-2	Checks to see if the information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.	Examine the user or group role structure that is set up within the GenTax® application. Verify access to functions or areas in GenTax® are protected by access controls.	The application enforces a separation of duty by restricting access to functions or areas within the GenTax application using a user or group role structure. Roles are assigned for a particular set of users and then that role/group is given only the rights that are required to perform that duty.			

Test ID	NIST ID (800-53)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
3	AC-5, AC-6	Checks to see if the information system enforces separation of duties through assigned access authorizations.	1. Interview the administrator to determine how user and group access is assigned. 2. Examine the accounts granted direct DBMS access to execute queries. 3. Examine the accounts granted access to the GenTax Configuration Tool.	1. User and group access is assigned using the principle of least privilege by job function and need-to-know. Verify the user or group structure separates privilege levels for personnel that create, modify, and delete access control rules and personnel that perform either data entry or application programming. Verify the user or group structure separates privilege levels for personnel that review and clear audit logs and personnel that perform non-audit administration. Users listed, if any, with security equal to a "root user" are documented. 2. Direct access to the DBMS is restricted to database administrators only. 3. Access to the GenTax Configuration Tool is restricted to application administrators only.			

Test ID	NIST ID (800-53)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
4	AC-3	Checks to see if the information system enforces assigned authorizations for controlling access to FTI for only those accounts necessary	1. Verify security setting specifically for Data Warehouse manager: [GTREF] select fintFunction from rfrManager where fstrManager = 'Dwh' or GenTax TOOLS, Reference Editor 2. Verify security on individual data stores in Data Warehouse manager. Function #'s returned evaluated for how restrictive its policy is. [GTGLB] select fstrDataStoreName, fstrDescription, flngFunction from tblDWhDataStore where flngVer=0 and fblnActive=1 and fdtmProductionLoaded<'31-Dec-9999' *Note above query will return all datastores defined in the data warehouse, some of which may not be FTI sourced. Only look at FTI datastores. The name or description of the datastore will identify if it is an FTI datastore.	Access to the Data Warehouse Manager and the individual FTI data stores is restricted to authorized agency personnel with a valid need-to-know and a job function that requires access to FTI.			

Test ID	NIST ID (800-53)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
5	AC-4	Checks to see if the information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	Verify the controls in place within the GenTax® application and the supporting DBMS to ensure the flow of FTI through the application is properly controlled and FTI is properly identified.	It is recommended that FTI be kept separate from other information to the maximum extent possible to avoid inadvertent disclosures. Agencies should strive to avoid maintaining FTI as part of their case files. In situations where physical separation is impractical, the file should be clearly labeled to indicate that FTI is included and the file should be safeguarded. If FTI is displayed on screen as part of any GenTax report, the FTI is clearly labeled. If FTI is electronically transmitted from GenTax across the agency Local Area Network (LAN) or Wide Area Network (WAN), it is identified as FTI in the file name, and is not sent in the clear.			
6	AC-7	Failed Login Minimum Requirement	1. If LDAP off: [GTREF] select fintLoginAttempts from rfrPasswordConfig or GenTax TOOLS, Reference Editor If LDAP is used the GenTax® application relies on the control implemented by Windows Active Directory. The Account Lockout setting will need to be verified on the Windows AD Domain Controller.	fintLoginAttempts < 3 User account lockout feature disables the user account after 3 unsuccessful login attempts. Account lockout duration is permanent until an authorized system administrator reinstates the user account.			

Test ID	NIST ID (800-53)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
7	AC-8	Checks to ensure the IRS approved login banner is used.	1. Start GenTax® 2. Enter valid user id and authentication values for logon 3. Review legal notice on startup screen.	The legal notice warning banner is displayed prior to login, and contains the following IRS-approved language: WARNING This system may contain Government information, which is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of this computer system or of the data contained herein or in transit to/from this system constitutes a violation of Title 18, United States Code, Section 1030, and may subject the individual to Criminal and Civil penalties pursuant to Title 26, United States Code, Sections 7213, 7213A (the Taxpayer Browsing Protection Act), and 7431. This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording and analysis of all data being communicated, transmitted, processed or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to Law Enforcement Personnel. ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITO			

Test ID	NIST ID (800-53)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
8	AC-12	Checks to ensure the application automatically terminates a remote session after 15 minutes of inactivity.	Note: GenTax is a stateless application, therefore there is no continuous interacation with the application server that would require a connection timeout. Most agencies perform remote access to GenTax® through Remote Desktop sessions. The application can be made available over the Internet by installing an executable on the client. The application may also be accessible through a corporate VPN. If GenTax® is available over the Internet, verify if remote sessions are automatically terminated after 15 minutes of inactivity.	Remote sessions are automatically terminated after 15 minutes of inactivity.			
9	AC-14	Checks to see if the organization identifies and documents specific user actions that can be performed on the information system without identification or authentication	Attempt to access any module of the GenTax® application without logging in.	No actions can be performed within GenTax® without user identification and authentication first being required.			
10	AC-17	The agency authorizes, monitors, and controls all methods of remote access to the information system.	Verify the mechanism used for remote access to the GenTax® application. Note: Most agencies perform remote access to GenTax® through Remote Desktop sessions. The application can be made available over the Internet by installing an executable on the client. The application may also be accessible through a corporate VPN.	The remote access mechanism provides the following controls: All remote access to the application over the Internet is authorized and documented. Remote access connections are audited, and included in the application's audit trail. Remote access sessions are encrypted.			

Test ID	NIST ID (800-53)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
11	AU-2, AU-3, AU-8	Checks to ensure successful and unsuccessful login and logout activity is logged.	1. [GTSYS] select * from tblUserLog or GenTax TOOLS, Login Activity 2. [GTSYS] select * from tblUserLog where fdtmLogOff = fdtmLogOn or GenTax TOOLS, Login Activity	1. Successful logins and logouts are logged. 2. Unsuccessful logins are logged. 3. Time stamps (including date and time) of audit records are generated using internal system clocks.			
12	AU-2, AU-3, AU-8	Check to ensure FTI data access via the information system is being logged appropriately.	[GTSYS] select * from tblTableLog where fblnFederal=1 or GenTax TOOLS, Table Log Activity	1. FTI data store access authorizations are tracked and reviewed. 2. Time stamps (including date and time) of audit records are generated using internal system clocks.			
13	AU-4, AU-5, AU-11	The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	1. Review example log tables [GTSYS] select * from tblUserLog select * from tblUser select * from tblTableLog or GenTax TOOLS, Login Activity or GenTax TOOLS, Table Log Activity 2. Verify there is a mechanism in place to notify the administrator in the event audit logs near storage capacity, or the audit process has failed. Examine automated alerts that have been previously received by the administrator. 3. Verify the duration audit logs are retained in archive.	1. Complete log history is maintained in DBMS in appropriate table(s). Allocation storage is maintained as part of DBMS maintenance. Audit security logs are archived to a central log server. 2. There is an automated mechanism in place to ensure the administrator is notified when the application logs are near capacity, or when the application audit process has failed or has an error condition. The administrator has configured the percentage full at which the audit trail must be for this notification to be triggered. 3. To support the audit of activities, all agencies must ensure that audit information is archived for six years to enable the recreation of computer-related accesses to both the operating system and to the application wherever FTI is stored.			

14	AC-13, AU-6	Checks to see if table and/or security logs are reviewed on a periodic basis.	Verify table and/or security logs are reviewed on a daily basis for: - logon attempt failures by user - logons at unusual/non-duty hours - access to restricted system or data files indicating a possible pattern of deliberate browsing - System failures or errors - Unusual or suspicious patterns of activity [GTSYS] select * from tblTableLog select * from tblUserLog or GenTax TOOLS, Login Activity or GenTax TOOLS, Table Log Activity	Agencies routinely review audit records for indications of unusual activities, suspicious activities or suspected violations, and report findings to appropriate officials for prompt resolution.			
15	AU-9	Checks to see if the information system protects audit information and audit tools from unauthorized access, modification, and deletion.	1. Locate the table(s) that store the application audit log files within the DBMS. Examine the properties of the log files. 2. Verify the table permissions to ensure read, write and delete access is only granted to personnel responsible for maintaining and reviewing the audit logs.	1. The application does not permit modification of logged or historical information. 2. Access to the application audit logs is restricted to personnel responsible for maintaining and reviewing the audit logs (e.g., security administrator).			
16	IA-2	The application uniquely identifies and authenticates users.	1. Attempt to login to the application leaving the user name and password fields blank. 2. Attempt to login to the application with a valid user name and leave the password field blank.	All login attempts fail. Identification and authentication is required in order to access the application. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof.			
17	IA-5	Checks to see if the agency uses the GenTax® configuration or the LDAP configuration for authentication controls.	[GTREF] select fblnUseLDAP from rfrPasswordConfig or GenTax TOOLS, Reference Editor	If result/flag set to TRUE then GenTax® is using LDA and relies on the controls provided by the Windows Active Dircetory.			Note: If LDAP is used, the Windows Active Directory settings need to be tested for the procedures where the test steps note.

Test ID	NIST ID (800-53)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
18	IA-5	Agency has defined appropriate rules for password management in GenTax® (e.g. length, numeric, mixed case, etc.)	If LDAP off, verify password configuration strength based on number of column settings on rfrPasswordConfig: [GTREF] select * from rfrPasswordConfig - fintMinLength - fblnRequireNumeric - fblnRequireMixedCase - fblnRequireOther - fblnNoUserIDAsPwd - fblnPasswordReuseAllowed or GenTax TOOLS, Reference Editor If LDAP is used the GenTax® application relies on the control implemented by Windows Active Directory. The password minimum length, complexity and history settings will need to be verified on the Windows AD Domain Controller.	Passwords are a minimum length of 8 characters in a combination of alpha and numeric or special characters.			
19	IA-5	The information system shall routinely prompt users to change their passwords within 5-14 days before such password expires.	If LDAP off: [GTREF] select flngPWDExpireDaysToNotify from rfrPasswordConfig or GenTax TOOLS, Reference Editor If LDAP is used the GenTax® application relies on the control implemented by Windows Active Directory. The password change warning setting will need to be verified on the Windows AD Domain Controller.	The application prompts users to change their passwords within 5-14 days before such password expires.			

Test ID	NIST ID (800-53)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
20	IA-5	Users shall be prohibited from using their last six passwords to deter reuse of the same password.	If LDAP off: [GTREF] select fintNumberOfRequired from rfrPasswordConfig or GenTax TOOLS, Reference Editor Verify password history maintained: [GTSYS] select fstrUser,fstrPassword from tblUser where flngVer<>0 If LDAP is used the GenTax® application relies on the control implemented by Windows Active Directory. The password history setting will need to be verified on the Windows AD Domain Controller.	Users are prohibited from using their last six passwords to deter reuse of the same password.			
21	IA-5	Maximum Password Age is enforced.	If LDAP off: [GTREF] select flngPWDExpireDays from rfrPasswordConfig or GenTax TOOLS, Reference Editor If LDAP is used the GenTax® application relies on the control implemented by Windows Active Directory. The maximum password age setting will need to be verified on the Windows AD Domain Controller.	flngPWDExpireDays <= 90 (standard users) flngPWDExpireDays <= 60 (privileged users) Passwords are changed every 60 days, at a minimum, for privileged user accounts, and every 90 days for standard user accounts.			
22	IA-5	Minimum Password Age is enforced.	GenTax® v6 does not have the capability to enforce a minimum password age if the LDAP is off. If LDAP is used the GenTax® application relies on the control implemented by Windows Active Directory. The minimum password age setting will need to be verified on the Windows AD Domain Controller.	Users shall be prohibited from changing their passwords for at least 15 days after a recent change. Meaning, the minimum password age limit shall be 15 days after a recent password change.			

23	IA-5	Password Expiration is configured properly.	Select one or more defined GenTax® users and navigate to their security profile screen to verify the "password never expire" option is not checked. 1. This test is to verify that password expiration is enabled. [GTSYS] select * from tblUser where flngVer = 0 and fdtmStart < GetDate() and fdtmEnd > GetDate() and fblnPasswordNeverExpires = 1 2. This test is for any active user who's password expire date is greater than 60 (non-privileged user) or 90 (privileged user) days. Change the parameter in the command to 60 for non-privileged users. [GTSYS] Select * from tbluser where flngver = 0 and fdtmend = '9999-12-31 00:00:00.000' and fdtmPasswordExpires > dateadd(day,90,Getdate()); If LDAP is used the GenTax® application relies on the control implemented by Windows Active Directory. The "password never expires" setting will need to be verified on the Windows AD Domain Controller.	"Password never expire" box is not checked. The second command should return no outupt indicating there are no privileged accounts with a password expire date greater than 60 days and no non-privleged accounts with a password expire date greater than 90 days.			
24	AC-2	Checks to ensure all accounts have unique user names.	[GTSYS] select fstrUser,count(*) from tblUser where flngVer=0 group by fstrUser having count(*)>1	Every GenTax® application account name is unique. Accounts do not have the same user or account name.			

Test ID	NIST ID (800-53)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
25	IA-5	Checks to ensure new users must change their password upon initial login to the application.	1. Create a new demonstration user for test purposes. 2. Verify the following flag is set: '- new users default flag of "next logon change password" = True; 3. Login using the newly created test user account and verify the password change prompt.	1. The "next logon change password" flag is set to True. 2. The test user account is prompted for a password change upon initial login.			
26	IA-6	Check to see if the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	1. Verify during login to the application that the user's password is obscured on screen during input. 2. Force a bad login by entering an invalid password and observe the onscreen feedback.	1. Passwords are masked during input. 2. Invalid login reports message of bad login or password, thus not providing information of what was wrong (the password or the login).			
27	IA-7	Checks to ensure passwords are encrypted on the client, in transmission, and while stored in the DBMS	1. [GTREF] select fstrEncryptionType from rfrPasswordConfig or GenTax TOOLS, Reference Editor 2. [GTSYS] select fstrPwdEncryptionType, fstrPassword from tblUser	GenTax® supports SHAXXX password hashing. Passwords encrypted on tblUser within the DBMS Passwords are encrypted on the client, in transmission and while stored in the DBMS using NIST FIPS 140-2 validated encryption.			
28	SC-2	Checks to see if the information system separates user functionality (including user interface services) from information system management functionality.	Examine the GenTax® application architecture to determine how system management and user interface services are separated. Interview the application administrator or examine the application documentation to determine the location of the application code. Examine the directory where the application code is located.	The application data is not located in the same directory as the code. Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.			

Test ID	NIST ID (800-53)	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
29	SC-4	Checks to ensure the application prevents unauthorized and unintended information transfer via shared system resources.	Examine the system architecture and interview the system administrator to verify the application does not store FTI in a system cache, registers, main memory, or secondary storage after a user session is terminated.	Temporary files/objects that may contain FTI, including encrypted files, are not released to any system cache, registers, main memory or secondary storage when a user session is terminated.			
30	SC-13	Checks to ensure the application uses an approved cryptographic module.	If the application does not utilize encryption, key exchange, digital signature or hash, FIPS 140-2 cryptography is not required this check is not applicable. Verify that all cryptography functions used by the application are FIPS-140 validated cryptographic modules. The National Institute of Standards and Technology's FIPS 140-1 and FIPS 140-2 Vendor List is http://csrc.nist.gov/cryptval/.	The application uses approved FIPS 140-2 compliant modules.			
31	SC-23	Checks to ensure the application provides mechanisms to protect the authenticity of communications sessions.	Examine the system architecture and interview the system administrator to verify the protocol used for sessions between the client and server. Verify the protocol in use has the capability to authenticate the client and server during communication sessions.	The protocol in use provides an authentication mechanism for the communication sessions between client and server.			

IRS Safeguard SCSEM Legend	
Test Case Tab: Execute the test cases and document the results to complete the IRS Safeguard Computer Security review. Reviewer is required to complete the following columns: Actual Results, Comments/Supporting Evidence. Please find more details of each column below.	
Test ID	Identification number of SCSEM test case
NIST ID	NIST 800-53/PUB 1075 Control Identifier
Test Objective	Objective of test procedure.
Test Steps	Detailed test procedures to follow for test execution.
Expected Results	The expected outcome of the test step execution that would result in a Pass.
Actual Results	The actual outcome of the test step execution, i.e., the actual configuration setting observed.
Pass/Fail	Reviewer to indicate if the test case pass, failed or is not applicable.
Comments / Supporting Evidence	Reviewer to include any supporting evidence to confirm if the test case passed., failed on not applicable As evidence, provide the following information for the following assessment methods: 1. Interview - Name and title of the person providing information. Also provide the date when the information is provided. 2. Examination - Provide the name, title, and date of the document referenced as the evidence. Also provide section number where the pertinent information is resident within the document (if possible). Ensure all supporting evidence to verify the test case passed or failed. If the control is marked as NA, then provide appropriate justification as to why the control is considered NA.
Assumptions	Database level controls are not tested as part of this SCSEM. Queries executed against the database are for purposes of testing application level security controls, not database or DBMS level security controls.

Version	Release Date	Summary of Changes	Name
0.1	5/30/2008	First Release	Booz Allen
0.2	7/21/2008	Updated test ID #5 to include language from Pub 1075 on commingling. Added language to Test ID #8 note to clarify that GenTax is a stateless application.	Booz Allen
0.3	10/30/2008	Updated test ID #23 to include a second test step to test for the password expire interval.	Booz Allen